Module V: E-commerce Security and Payment Systems - Comprehensive Explanation

This document provides a comprehensive explanation of the topics covered in the "Module-V.ppt" presentation, focusing on the **E-commerce Security Environment** and **E-commerce Payment Systems**. All technical terms are presented with their full forms and abbreviations to aid in exam preparation.

---

1. The E-commerce Security Environment

The Internet provides opportunities for both legitimate business and **cybercrime**. The cost of cybercrime is significant, including direct losses, security expenses, and reputational damage.

1.1. Risks and Multilayered Security

E-commerce involves risks similar to traditional commerce, such as theft, fraud, and loss of privacy. **E-commerce security** is a complex, multi-layered process that requires a combination of:

- **Technologies and Tools:** Encryption, firewalls, **IDS** (Intrusion Detection Systems).
- **Organizational Policies:** Establishing and enforcing security procedures.
- **Legal and Industry Standards:** Adhering to laws and standards like **PCI-DSS** (Payment Card Industry - Data Security Standard).

Note: Perfect security is not achievable; the goal is to manage and minimize risks. Security is only as strong as its **weakest link**, which is often human error.

1.2. Dimensions of E-commerce Security

E-commerce security aims to protect six key dimensions:

Dimension	Description	Example of Protection
Integrity	Ensures information is not altered by unauthorized parties during transmission or storage.	Preventing unauthorized changes to a bank wire transfer amount.
Nonrepudiation	Ensures E-commerce participants cannot deny their online actions.	Preventing a customer from denying they placed an order.
Authenticity	Verifies the identity of individuals or entities in online interactions.	Verifying that a website operator is who they claim to be (preventing "spoofing").
Confidentiality	Ensures messages and data are only accessible to authorized individuals.	Safeguarding sensitive customer information from unauthorized access.
Privacy	Involves controlling the use of customer information provided to merchants.	Internal policies governing how customer data is collected, stored, and used.
Availability	Ensures that E-commerce sites function as intended and remain accessible to users.	Protecting the website from **DDoS** (Distributed Denial of Service) attacks.

1.3. Security Threats

Common security threats in the E-commerce environment include:

- **Botnet Attacks:** Networks of compromised computers used to launch attacks.
- **DDoS Attacks:** Overwhelming a server with traffic to make a website unavailable.
- **Trojans:** Malicious software disguised as legitimate programs.
- **Phishing:** Deceptive attempts to acquire sensitive information (e.g., usernames, passwords) by masquerading as a trustworthy entity.
- **Ransomware:** Software that blocks access to a computer system until a sum of money is paid.
- **Online Credit Card Fraud:** Criminals stealing and using credit card details, often in **CNP** (**Card Not Present**) transactions.

2. E-commerce Payment Systems

Online payments are a critical component of E-commerce, with credit and debit cards remaining the primary form of payment in many regions.

2.1. Modes of Electronic Payments

Electronic Payment refers to paperless monetary transactions, which reduce paperwork, transaction costs, and labor costs. Key modes include:

- **Credit Card:** A small plastic card with a unique number linked to an account. The card issuer bank pays the merchant on behalf of the customer, who then pays the bill later.
- **Debit Card:** A card that deducts money directly from the customer's bank account.
- **Smart Card:** Similar to a credit card but with an embedded **microprocessor chip** that stores customer information and money. They are accessed using a **PIN** (Personal Identification Number).
  - **Relationship-based Smart Card:** Enhances existing card services (e.g., access to multiple accounts).
  - **Electronic Purses:** Wallet-sized cards that store a sum of money for use instead of cash.
- **E-Money:** Digital representation of value.
- **EFT** (**Electronic Fund Transfer**): The electronic transfer of money from one bank account to another.

2.2. Credit Card Payment Process

The process involves several key actors:

1. **Card Holder** (Customer)
2. **Merchant** (Seller)
3. **Card Issuer Bank** (Customer's bank)
4. **Acquirer Bank** (Merchant's bank)
5. **Card Brand** (e.g., Visa, MasterCard)

The transaction process involves:

1. Customer presents card details (often encrypted).
2. Merchant validates identity and relays charge information to the Acquirer Bank/Processor.
3. Processor relays to the Card Brand (e.g., VisaNet, Banknet).

4. Card Brand relays to the Issuer Bank for authorization.
5. Authorization is returned to the Merchant.

2.3. Alternative Online Payment Systems

These systems address the limitations of credit card payments (security, high costs, accessibility).

- **Payment Enablers/Processors:** Services like Authorize.net, Cashfree, PayU, and Razorpay help merchants process credit card payments.
- **Alternative Systems:** PayPal, Amazon Pay, Visa Checkout, MasterPass.

2.4. Mobile Payment Systems

Mobile payments, facilitated by **mobile wallet apps**, are the fastest-growing alternative method.

- **Universal Proximity Wallets:** Used at various merchants via technologies like **NFC** (Near-Field Communication) (e.g., Apple Pay, Google Pay, Samsung Pay).
- **Branded Store Proximity Wallets:** Used only at a single merchant (e.g., Walmart, Starbucks apps).
- **P2P** (**Peer-to-Peer**) **Apps:** Used for payments between individuals (e.g., Venmo, Square Cash).

2.5. Blockchain and Cryptocurrencies

- **Blockchain:** A decentralized, distributed ledger technology that enables secure and transparent transactions.
- **Cryptocurrencies:** Digital or virtual currencies that are secured by cryptography (e.g., Bitcoin).
- **Altcoins:** Alternative cryptocurrencies to Bitcoin.
- **ICOs** (**Initial Coin Offerings**): A method for startups to raise capital by issuing cryptocurrency tokens.

This comprehensive overview should provide a strong foundation for your exam preparation on Module V. Good luck!